Cisco

642-544

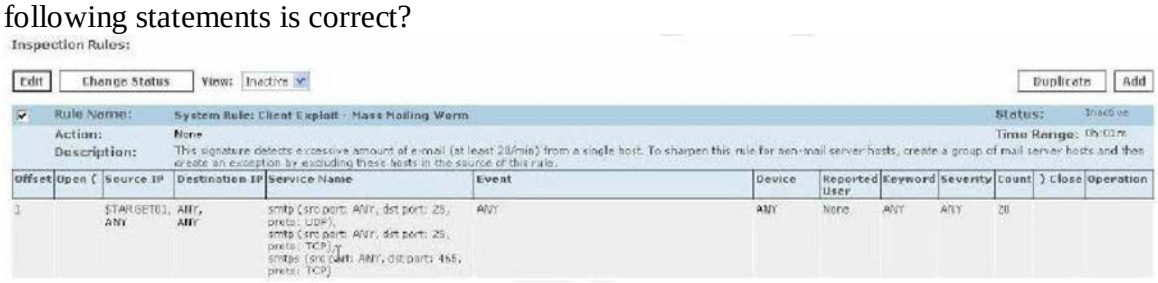
Implementing Cisco Security Monitoring, Analysis and Response

Refering to the rule shown on the MARS GUI screen, which two of the following statements are correct?(Choose two.)

A. This rule will fire if the offset 1 condition occurs "OR" if the offset 2 condition occurs.
B. This rule will fire if the offset 3 condition occurs.
C. The expressions between cells are "AND' while the expressions between items in the same cell are "OR".
D. This is a user-defined rule.
E. This rule can be deleted after changing its status to "inactive."

Answer: B, C

QUESTION: 42
Referring to the System Inspection Rule shown on the MARS GUI screen, which one of the following statements is correct?



A. Click on "Add" to activate the rule.
B. Click on "Activate" to activate the rule.
C. Click on "Change Status" to activate the rule.
D. Click on "Edit." Then you can apply and activate the rule.
E. Click on "Duplicate" to archive the rule to a remote NAS.

Answer: C

QUESTION: 43
Referring to the diagram shown on the MARS GUI screen, why is the Push function not enabled (grayed out)?

Enforcement Device: **HQ-FW-1**, Alternate

Default gateway: 172.30.1.1

Enforcement Device Information

Device	Type	Manager	Children	Log To	Collects From
HQ-FW-1	Cisco PIX 6.2	PN-MARS on demo3		PN-MARS on demo3	

Interface Information

Direction	IP Address	Interface Name	DNS Name	MAC Address	MAC Update Time
Inbound	10.33.10.2	inside	None / not found.	N/A	N/A
Outbound	192.168.1.1	DMZ-slot:1	None / not found.	N/A	N/A

Recommended Policies/Commands

```
access-list inside-acl
  deny tcp host 10.1.1.10 host 192.168.1.10 eq 21
```

Or

```
access-list inside-acl
  deny tcp host 10.1.1.10 any
```

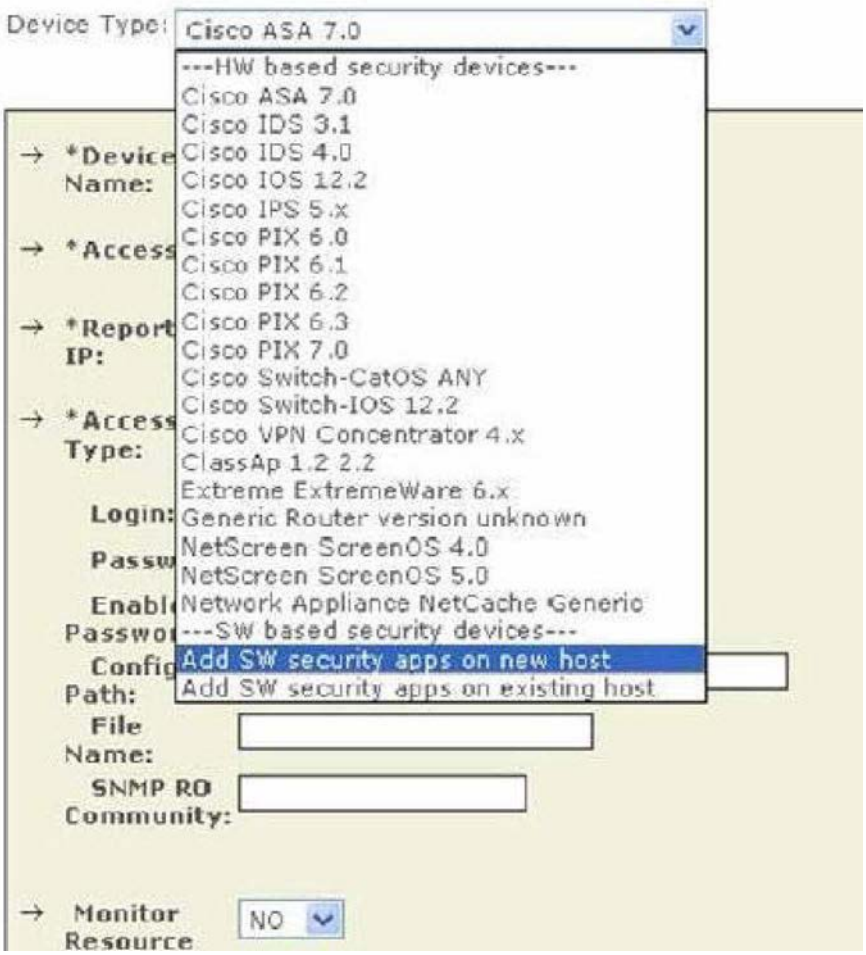
Or

```
shun 10.1.1.10 192.168.1.10 4002 21 tcp
```

A. Because the HQ-FW-1 device is the alternate choke point for mitigating this attack.
B. Because MARS cannot push commands to Layer 3 devices.
C. Because the Incident has not been confirmed by the administrator.
D. Because the Incident is a false positive.
E. Because MARS is operating at level 2 and not at level 3.
F. Because the selected mitigation command is not supported on the HQ-FW-1 device.

Answer: B

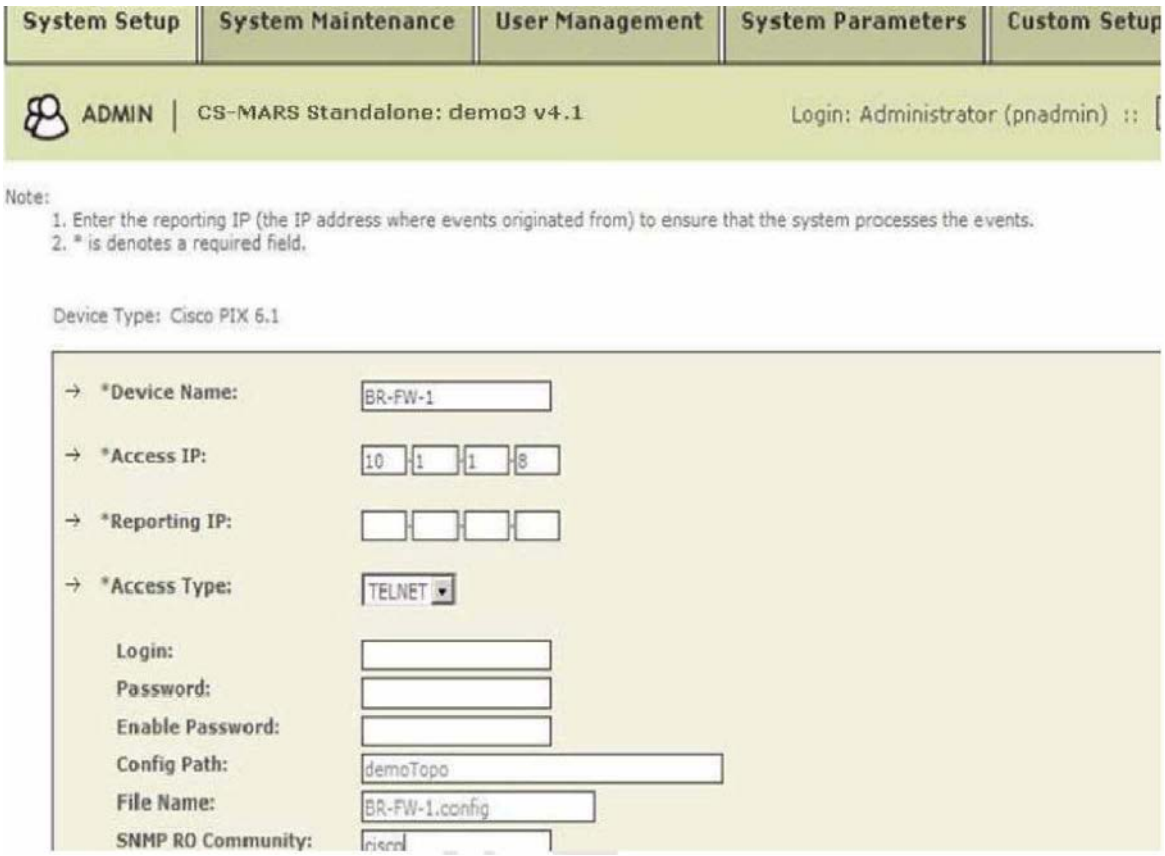
QUESTION: 44
Which three of the following reporting devices can be added to the MARS appliance using the "Add SW security apps on new host?" (Choose three.)



A. Cisco ACS
B. Netflow
C. SNORT
D. FWSM
E. Generic web server.

Answer: A, C, E

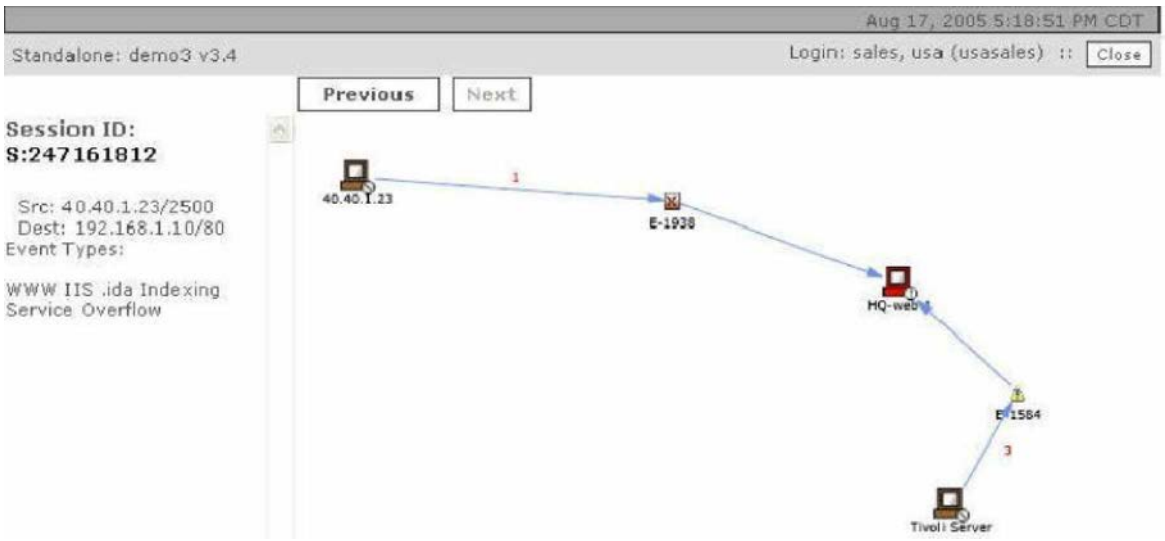
QUESTION: 45
After manually adding the BR-FW-1 device shown in the MARS GUI screen, what additional steps do you need to perform?



A. Click "Activate" to enable the device.
B. Click "Submit" to enable the device.
C. Click "Submit" to test access to the device. When access is successful, click "Activate" to activate the device.
D. Click "Activate" to activate the device, then click "Submit" to save the device configuration.
E. Click "Discover' to initiate manual discovery. When discovery is completed, click "Submit," then "Activate."

Answer: E

QUESTION: 46
Referring to the incident Vector Graph shown on the MARS GUI screen, which three of the following statements are correct? (Choose three.)



A. The port being attacked is port 80.
B. This incident has two associated Event Types.
C. You can mitigate this attack by clicking on the device being attacked.
D. The device being attacked is the Tivoli Server.
E. Click the Previous button to view any other Sessions related to this incident.

Answer: A, B, E

QUESTION: 47
Referring to the Rule shown on the MARS GUI screen, what is used to determine that three is a sudden traffic increase to a particular port, and which type of attack is this Rule useful for detecting? (Choose two.)

Rule Name:	System Rule: Sudden Traffic Increase To Port
Action:	None
Description:	This rule detects scans statistically significant increase in traffic to a particular port.

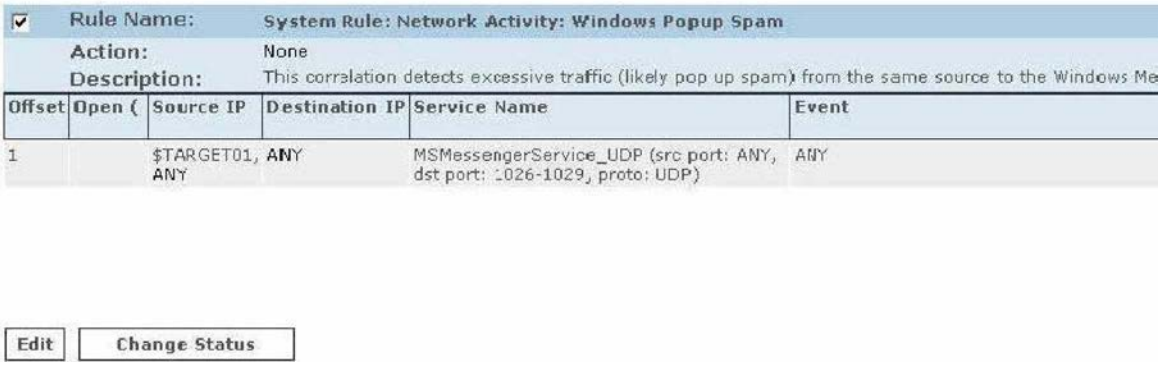
Offset	Open (	Source IP	Destination IP	Service Name	Event	Device
1		ANY	ANY	ANY	Sudden increase of traffic to a port	ANY

A. Ral-time queries
B. CSA logs
C. Netflow data
D. Smp polling
E. Dy-zero attacks
F. Acess attacks
G. Reconnaissance attacks
H. Denial of service attacks.

Answer: C, E

QUESTION: 48

To configure the MARS appliance to send out an alert when the system rule fires, what should you do from the MARS GUI screen shown?

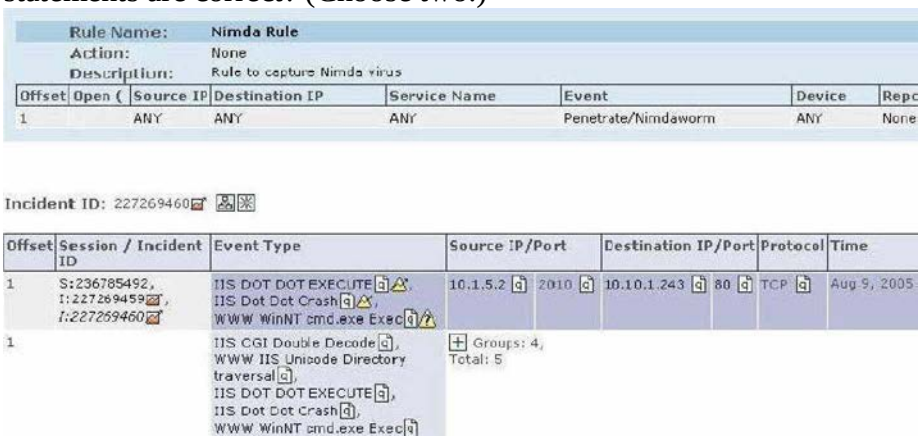


A. Click on "Active" in the "Status" field, select the appropriate alerts, then apply.
B. Click on "None" in the "Action" field, select the appropriate alerts, then apply.
C. Click "Edit" to edit the "Operation" field of the rule, select the appropriate alert option(s), then apply.
D. Click "Edit" to edit the "Event" field of the rule, select the appropriate alert option(s), then apply.
E. Click "Edit" to edit the "Reported User" field of the rule, select the appropriate alert option(s), then apply.

Answer: B

QUESTION: 49

Referring to the incident shown on the MARS GUI screen, which two of the following statements are correct? (Choose two.)



A. This is a low-severity incident.

B. This is a false positive incident.
C. There are multiple events that correlate to the 236785492 session.
D. The 236785492 session is related to both the 227269459 and the 227269460 Incidents.
E. The Nimda rule triggered both the 227269459 and the 227269460 Incidents.

Answer: C, D

Download Full Version From https://www.certkillers.net

Pass your exam at First Attempt....Guaranteed!